UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/343,464	06/30/1999	STEVEN M. BELLOVIN	2685/113031	7948

26652 7590 08/11/2003

AT&T CORP.
P.O. BOX 4110
MIDDLETOWN, NJ 07748

EXAMINER
FIELDS, COURTNEY D

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 08/11/2003

9

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/343,464	BELLOVIN, STEVEN M.	
	Examiner	Art Unit	
	Courtney D. Fields	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-22, 29-31 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

Response to Amendment

Claim Rejections - 35 USC § 112

1. Corrections made in regards to Claim 22 has been received and accepted. The rejection has been withdrawn.

Response to Arguments

1. Applicant's arguments filed 6/2/2003 have been fully considered but they are not persuasive.

2. Referring to the rejection of claims 1 and 11, the Applicant argues that Williams does not disclose the limitation of "authenticating an identifier for said packet". The Examiner disagrees and asserts that Williams does teach authenticating information sent between a host and a principal where the identifying information is found in the IP addresses. The NSC was designed to configure and audit the secure network and a network security device. The NSC is a dedicated machine that is responsible for both authenticating principals when they connect to the network and for authorizing connections. The NSC is contacted to verify the authentication data. (See Column 17, lines 66-67, Column 18, lines 1-19) As shown in the example, embodiment of Column 26, lines 1-64, Williams teaches that the security officer at the NSC is used to set up permitted associations between hosts based on IP addresses. Williams also teaches the ability of defining multiple permitted profiles for a principal, which will determine if the communication should be established between the principal and the host. Referring to claims 2 and 12, the Applicant argues that Williams does not teach the steps of "comparing said identifier to a list of identifiers and determining whether to send

said packet"... in accordance with such a comparison and at least one policy rule". The Examiner disagrees and asserts that Williams teaches the method of a network enforcing the discretionary access control policy based on hardware addresses, IP addresses, and TCP/UDP ports. (See Column 15, lines 40-57)

The network also provides port filtering based on TCP/UDP ports. The ports are used to identify specific endpoints on the sending and receiving hosts. Port filtering rules are part of the DAC security policy that serves as a means to further restrict communication between pairs of hosts that are authorized to communicate with one another. If the protocol type does not specify which specific port, then the packet is passed to IP filtering and is rejected because of a host-to-host association or a blocked port. (See Column 15, lines 66-67, Column 16, lines 1-25)

Referring to claims 3 and 13, the Applicant argues that Williams does not disclose the usage of "common host identifiers". The Examiner disagrees and asserts that common host identifier according to the Applicant's Specification is defined as being an IP address or a port number. Williams clearly teaches the limitation of using an NSC to provide real-time alarms of attempted security violations directed towards IP addresses, protocol type and port number. This will prevent the offending host from gaining access to the network. (See Column 17, lines 28-35)

Referring to claims 4 and 14, the Applicant argues that Williams does not disclose the limitation of "wherein said authenticating is performed in accordance with IPSEC standards". The Examiner disagrees and contends that Williams teaches the means of authenticating data between two hosts by using a device to transmit authenticating data

in which a shared secret is one of the possible mechanisms. The approved mechanisms used are defined in the IPSEC standards. (See Column 25, lines 37-63)

Referring to claims 5 and 15, the Applicant argues that Williams does not disclose the limitation of using a key to authenticate the packet, and not encrypt the packet. The Examiner disagrees and contends that Williams teaches during the installation of security device functions, the administrator is authenticated through the authentication interface unit and can have access to the IP addresses, nodes, NSC, default routers, and a cipher key. (See Column 20, lines 41-46)

Referring to claims 6 and 16, the Applicant argues that Williams does not disclose authentication or the sending of a message to a third device when an identifier is determined to be authentic. The Examiner argues and contends that Williams uses a MAC security policy for verifying if the packet is consistent with the receive security window. The security device verifies the integrity of the received packet by calculating a message digest, if the computed values match the value sent by the originating security device, then the packet was not modified. If the values does not match, an audit is generated using NSC security device, and the processing flow is terminated. (See Column 23, lines 8-16)

Referring to claim 21, the Applicant argues that Williams does not disclose a "first memory segment containing a list of common host identifiers".

The Examiner disagrees and contends that Williams discloses a CPU using a transmit association list located in the internal memory by performing DAC for determining if the destination IP addresses is in the transmit list. (See Column 21, lines 59-61)

It is known in the art, that an IP address can be defined as a common host identifier.

Referring to claim 29, the Applicant argues that Shwed nor Williams discloses a means for authenticating a packet.

The Examiner disagrees and contends that the combination of William's teachings combined with Shwed's teachings does disclose the means of authenticating a packet. Specifically, Williams teaches the security device will only send and receive messages if the communication has been authorized. Each message will be encrypted before transmission and decrypted before arrival to its destination in Column 8, lines 46-57.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) do not apply to the examination of this application as the application being examined was not (1) filed on or after November 29, 2000, or (2) voluntarily published under 35 U.S.C. 122(b). Therefore, this application is examined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

2. Claims 1-28 are rejected under 35 U.S.C. 102(e) as being anticipated by Williams U.S. Patent No. 6,304,973. Referring to claims 1 and 11, Williams discloses a method and system comprising:

a. Receiving a packet from one device to a second device (See Column 21, lines 22-24, and Column 23, lines 1-2)

b. Authenticating an identifier for the packet (See Column 23, lines 2-7)

c. Determining if packet should be sent to the second device (See Column 23, lines 10-15)

d. Sending packet to second device (See Column 23, lines 17-20)

Referring to claims 2 and 12, Williams discloses the claimed limitation of comparing identifier to a list of identifiers, retrieving at least one policy, and determining if packet should be sent to the second device in Column 21, lines 59-67, and Column 22, lines 1-3.

Referring to claims 3 and 13, Williams discloses the claimed limitation of identifier being a host identifier in Column 23, lines 28-33.

Referring to claims 4 and 14, Williams discloses the claimed limitation of authenticating in accordance with IPSEC standards in Column 11, lines 60-67.

Referring to claims 5 and 15, Williams discloses the claimed limitation of retrieving security from authentication header, retrieving a key with security, and determining if packet is authentic using a key in Column 11, lines 5-36 and Column 12, lines 1-3.

Referring to claims 6 and 16, Williams disclose the claimed limitation of sending a message to a device indicating that identifier is not authentic in Column 16, lines 15-36.

Referring to claims 7 and 17, Williams disclose the claimed limitation of having an IPSEC authentication header in Column 9, lines 36-41.

Referring to claims 8 and 18, Williams discloses the claimed limitation of having an packet encrypted before receiving it and further decrypting packet before authentication in Column 22, lines 33-44, 48-51.

Referring to claims 9 and 19, Williams discloses the claimed limitation of encrypting and decrypting a packet by using DES and triple DES in Column 9, lines 21-28.

Referring to claims 10 and 20, Williams discloses the claimed limitation of having a policy stored in a file in a second device in Column 15, lines 41-57.

Referring to claim 21, Williams discloses the claimed limitation of having input coupled to a network for receiving a packet in Column 19, lines 66-67 and Column 20, lines 1-4, a first buffer coupled to input for storing packet in Column 24, lines 57-67, memory containing a list of identifiers (profiles) in Column 25, lines 37-46, another memory for storing decryption of packets in Column 24, lines 48-54, a processor coupled to first buffer in Column 17, lines 41-46, and a output for forwarding packet to second device in Column 21, lines16-21.

Referring to claim 22, Williams discloses the claimed limitation of having a second buffer for storing packets in Column 24, lines 34-38.

Referring to claim 23, Williams discloses the claimed limitation of having random access memory in Column 19, lines 66-67, Column 20, lines 1-4.

Referring to claim 24, Williams discloses the claimed limitation of having a non-volatile random access memory in Column 19, lines 59-61.

Referring to claim 25, Williams discloses the claimed limitation of receiving a list of addresses in Column 21, lines 59-64.

Referring to claim 26, Williams discloses the claimed limitation of receiving a terminal and a serial port in Column 15, lines 66-67 and Column 16, lines 1-8.

Referring to claim 27, Williams discloses the claimed limitation of receiving a network interface card in Column 6, lines 53-57.

Referring to claim 28, Williams discloses the claimed limitation of having a wireless network for receiving packets in Column 12, lines 56-67.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claim 29 is rejected under 35 U.S.C. 103(a) as being unpatentable over Williams in view of Shwed U.S. Patent No. 5,606,668. Referring to claim 29, Williams teaches the means of providing cryptographic techniques as a method of authenticating the identity of each sender, before encrypting and decrypting each packet. However, Williams does not teach the means for a distributed firewall system comprising a system management module and a packet filter processor. Shwed teaches the claimed limitation of having a first network device in Column 3, lines 27-31, a second network device in Column 3, lines 31-35, a packet filter for each network device in Column 3, lines 59-65, and a system administrator control module to manage packet filters in Column 3, lines 44-48

and Column 4, lines 30-37. Accordingly, it would have been obvious to a person of ordinary skill in the art, at the time the invention was made to incorporate packet filtering in a distributed firewall, which allows network security to be more controllable when communicating through a data packet. Furthermore, one of ordinary skill in the art would have been motivated to do this since, a need exists for a secure method and system that supports data packets in a public network which prevents unauthorized usage.

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 703-305-8293. The examiner can normally be reached on Mon - Thu 7:00 - 5:00 pm; off every Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone numbers

for the organization where this application or proceeding is assigned are 703-746-7239 for regular communications and 703-746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

CDF

cdf
August 7, 2003

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100